September 2011 SwA Forum
Addressing Software Risks Throughout the Supply Chain
September 12-16, 2011
SEI, Arlington VA

Monday September 12

Sub-Theme: "Protecting Against Predatory Practices"

Target Audience: Acquisition Support Decision Makers And Contracts Team Members

SEI Member Community: Acquisition Support

Session 1: Leadership Welcome

Speakers:

Howard A. Schmidt, Special Assistant to the President and the Cybersecurity Coordinator (via video)

Roberta "Bobbie" Stempfley, Acting Assistant Secretary, Cyber Security and Communications (CS&C) Department of Homeland Security

Session Overview

The increased dependency of both public and privte entities on technology coupled with an increasingly complex global supply chain has contributed to the emergence of software supply chains as threat vectors for cyber attacks. To mitigate risks attributable to exploitable software, organizations must understand how they could be attacked, how to identify the weaknesses in their software, and how to implement appropriate mitigation practices. Speakers in this session will share their perspectives and insights on Protecting Against Predatory Practices

Session 2: Acquisition Reform: Leadership In Balancing, Cost Schedule And Performance

Speakers:

- Ken Nidiffer, SEI
- Don Davidson, DoD CIO
- TBD, IT Acquisition Advisory Council
- Ron Pontius, OASD(NII)/DoD CIO

Session Overview

Numerous government efforts are focused on addressing the efficiency and effectiveness of government acquisition processes. This panel will provide insight into some of these efforts and explore the successes and challenges in addressing the complexity of the acquisition process and supply chain risks including the lack of transparency and traceability as well as standardized assurance and compliance policies throughout the acquisition lifecycle.

Welcome from Our Host

Paul Nielsen, Director and Chief Executive Officer of the Software Engineering Institute (SEI),

Session 3: Challenges with Trusted Business Partners

Speakers:

- Thresa Lang, Dell
- Randy Trzeciak, CERT/SEI
- Marc Spitler, Verizon
- Angela Mckay, Microsoft
- TBD, OTTF

Session Overview

According to the 2011 Verizon Data Breach report, approximately **50%** of data involved malware. Increased outsourcing of software development and software services exponentially increases number of people who touch software products and services during the acquisition process. This panel will provide insight into the challenges, lessons learned, and ongoing efforts to enable organizations to acquire trusted products from business partners.

Session 4: Addressing Community Perspectives In Practice Adoption

Speakers:

- Palma Buttles-Valdez, SEI
- Ian Bryant, UK Software Security, Dependability and Reliability Initiative (SSDRI)
- Marc Esteve, US-Crest
- David White, CERT/SEI

Session Overview

It can be challenging get a project tem to adopt a new set of practices. The global nature of the software assurance challenge creates a unique environment for driving needed changes across the software supply chain. This panel will share observations, lessons learned, and existing challenges in addressing community perspectives in software assurance practices across the supply chain.

September 2011 SwA Forum
Addressing Software Risks Throughout the Supply Chain
September 12-16, 2011
SEI, Arlington VA

Tuesday September 13

Sub- Theme: Software Assurance In the Operational Environment

Target Audience: CERT, Technical Cyberscope Stakeholders/ITSAC

SEI Member Community: Computer Emergency Response Team (CERT)

Session 1: Software Assurance And Security Automation Leadership Perspectives

Speakers:

- Rich Pethia, CERT/SEI
- Tony Sager, NSA
- Bruce W. McConnell, DHS

Session Overview

Leaders from the US Department of Homeland Security (DHS), the National Security Agency (NSA), and the Software Engineering Institute (SEI) will discuss how their organizations are working within the overall Federal Government strategy to significantly improve cyber security in the Federal Government as well as assist the private sector secure their system and networks. Key topics will include recent efforts to align US Government initiatives in cyber security, the role of automation and international standards and ways that the private sector can participate in these efforts.

Tuesday Session 2 - Defending Software Infrastructure

Speakers:

- Tom Millar, DHS
- Chad Dougherty, CERT/SEI

Session Overview

Resilient cyber security systems require automated defense including software vulnerability analysis, vulnerability discovery, and technical countermeasures for exploit mitigation. How should the defenders of our software infrastructure collaborate to create open languages for event data,

observable indicators and correlation rules to be shared by diverse families of cyber security systems? What are the ways these strategies, tactics, and standards could be leveraged to exchange information and better coordinate defense and countermeasures?

Session 3: Leveraging Automation to Enhance FISMA

Speakers:

- Doug Andre, DHS FNS
- Jon Baker, MITRE

Session Overview

To assess the nature and extent of vulnerabilities, organizations must first collect a consistent set of metrics. The Federal Government is seeking to accomplish this with the CyberScope Initiative, which mandates Federal Civilian Agencies to report cyber security data using standardized formats. The CyberScope application is a web-based interactive tool that allows Federal Civilian Agencies to report data that complies with Federal Information Security Management Act (FISMA) rules. Ultimately, CyberScope will enable Federal Agencies to identify weaknesses and share information; thus improving the security of Federal cyber ecosystem.

Session 4: Bringing Operational Knowledge to Development

Speakers:

- Michele Moss, Booz Allen Hamilton
- Steve Lipner, SAFECode
- Bill Curtis, CISQ
- Rick Doten, Lockheed Martin
- Jeff Davenport, SEI

Session Overview

Provide insights into the advancement, opportunities, and challenges of leveraging incidents and forensics information to inform development and sustainment of trusted technology

September 2011 SwA Forum
Addressing Software Risks Throughout the Supply Chain
September 12-16, 2011
SEI, Arlington VA

Wednesday September 14

Track 1 – SwA at the Code Level Walt Houser	Track 2 – SwA Throughout the Lifecycle (Michele Moss)	Track 3– Securing Mobile Applications Jack Mannino & Walt Houser
Planning the Implementation of Attack-Aware Software with Active Defenses Colin Watson, Watson Hall Ltd	Building Security Into YOUR SDLC: Tailoring Industry Resources To Fit Your Organization Michele Moss, Booz Allen Hamilton Michael Konrad, SEI	Mobile Attack Implications Nicholas Percoco, Trustwave,
Dimensions of Static Analysis Based Assurance Mike Oara, Hatha Systems	SAFECode Security Development Lifecycle (SDL) Michael Howard, Microsoft Matthew Coles, EMC	OWASP Top 10 Mobile Risks Jack Mannino, nVisium Security
OMG Implementation Pattern Meta Model for Software Systems (IPMSS) Implications for Software Assurance Jason McColm Smith, The Software Revolution, Inc	OWASP Acquisition Language for Software Assurance Jeff Williams, Aspect Security	Mobile Applications Security Adam Meyers, SRA
Software Fault Patterns Nick Mansourov, KDM Analytics	Scalable Application Security Practices Jim Manico, WhiteHat Security	Security Testing Mobile Applications Dan Cornell, Denim Group

Track 1 – SwA at the Code Level

As the entire computer security industry is fully and painfully aware, applications are the #1 target for malicious attack. The root of this problem is vulnerable software -- trillions of lines worth of code and counting. On an internet-wide scale, how do we go about writing more secure code? How do we deal with the massive backlog of vulnerable code already in wide circulation? What are the best strategies for ensuring code remains secure as threats evolve?

Track 2 – SwA throughout the Lifecycle

Many organizations are struggling to find an approach to address today's need for increased confidence in our IT products and services. Fortunately, many of these same organizations have quality management practices in place to support achievement of their business goals. Successful software development approaches are based on recognized industry standards and best practices and designed to fit the needs and culture of the organization. Incorporating Software Assurance in the Lifecycle can be addressed in a similar way. The track will start with an overview of resources available to help organizations understand the strengths and weaknesses of their software assurance processes and develop a realistic roadmap to implement software assurance. Leading industry experts will provide deeper dives into key secure engineering practices, acquisition language for software assurance, and the use of software automation protocols in operations.

Track 3– Securing Mobile Applications

As mobile computing usage soars and gains deeper penetration into the enterprise, attackers are shifting gears to focus on the mobile platforms. The security and privacy implications of attacks against mobile platforms and applications presents great challenges to modern organizations. This track will cover the risks facing the mobile computing world and how we can proactively stay one step ahead of the bad guys. Presenters will outline the methods and approaches organizations and their developers need to take to protect their users and sensitive organizational data.

September 2011 SwA Forum
Addressing Software Risks Throughout the Supply Chain
September 12-16, 2011
SEI, Arlington VA

Thursday September 15

Sub Theme: Addressing Tomorrow (Education) & Yesterday (Legacy)Today

Target Audience AM: Education and Training PM: Research Community, Early Adopters

SEI Member Community: Research, Technology, and Systems Solutions

Session 1: The Educational Supply Chain: Addressing Today's SwA Knowledge Needs

Speakers:

- Mark Ardis, Stevens Institute of Technology
- Sajay Rai, Securely Yours, LLC
- John Heimann, Oracle
- Steve Lipner, Microsoft
- Nancy Mead, SEI

Session Overview

In today's environment we have too few personnel who are knowledgeable in software assurance for newly developed and acquired systems. Most of the training and degree program offerings focus on security of operational systems. Although the SwA curriculum project addresses this, we need to impact other curriculum development efforts and training efforts in order to bridge the gap. In this panel session we will discuss industry and government needs, as well as additional curriculum development efforts where software assurance could be addressed.

Session 2: The Educational Supply Chain: Defining The Vision For Building The Foundation For SwA Knowledge

Speakers:

- Peggy Maxson, DHS
- Karen Evans, U.S. Cyber Challenge
- Diane Burley , George Washington University
- Ian Bryant, UK Software Security, Dependability and Reliability Initiative (SSDRI), DeMontfort University
- Davina Pruitt, University of Maryland, CyberWatch Center

Session Overview

This panel addresses the question of strategic guidance. It will overview and examine the implications of a number of diverse trends and emerging factors in training and education for software assurance workers. These issues could all be influential in their potential long-term impacts and the development of workforce capabilities. The substantive directions they represent and the long-term outcomes will be presented and discussed

Session 3: Understanding the Impacts of Accurate Software Identification Across the Software Lifecycle

Speakers:

- Facilitator: Steve Klos, TagVault.org
- Pat Cicala, Cicala & Associates
- Roger Cummings , Symantec
- Larry Wagoner, NSA
- Richard Struse, DHS

Session Overview

Maintaining an accurate software inventory is vital to a well managed IT infrastructure. Accurately knowing that the software that you use has not been maliciously altered in the supply chain is necessary for a secure IT environment. All federal agencies and programs have a need to maintain accurate, authoritative and useful software identification information and the efforts to provide this data span across multiple entities. Learn why this job is so difficult, how the various efforts provide different benefits and how these efforts can be brought together to make an even stronger solution by leveraging an ISO/IEC standard that defines the requirements for software identification tags.

Session 4: Standards for SW Transparency

Speakers:

- Joe Jarzombek,DHS
- Jason McColm Smith, The Software Revolution, Inc
- Judith Klein, Lockheed Martin
- Mike Oara, Hatha Systems

Session Overview

Legacy systems are pervasive in today's critical infrastructure whether in banking, government, or healthcare. Legacy languages such as COBOL and its variants, assembler, Fortran, Pascal, C, C++, ADA, MUMPS and more are a significant part of our installed base with COBOL reaching as much as 1Trillion

lines of code. Java and VB have also reached the status of legacy languages. This panel will discuss the issues that exist in maintaining, upgrading and meeting compliance requirements for these legacy systems while addressing assurance needs. Client business/operational needs, standards, motivations for retaining the legacy languages will be discussed along with how assurance can play a big part in improving the state of legacy systems.

September 2011 SwA Forum
Addressing Software Risks Throughout the Supply Chain
September 12-16, 2011
SEI, Arlington VA

Friday September 16

Sub Theme: Enabling Successful Development Efforts: Standards, People, and Culture

Target Audience: Org Process/Governance and Lifecycle Standards

SEI Member Community: Software Engineering Process Management Program

Session 1: Enabling Successful Development Efforts: Standards, People, and Culture: The Enterprise Perspective

Speakers:

- Doug Schmidt, SEI
- Brian P. Gallagher, Northrop Grumman Information Systems (invited)
- Paul Croll, CSC

Session Overview

Speakers will share lessons learned and highlight special considerations from the enterprise perspective on enabling successful development efforts.

Session 2: Implementing SwA Practices During the Lifecycle Processes

Speakers:

- Toward a Trusted Supply Chain - Ralph Hood, Microsoft
- Securing Systems Through Software Reliability Engineering - Taz Daughtrey, Quanterion Solutions
- A Case Study in Integrated Security in the SDLC - Gordon Uchenickn, Coverity

Wrap up and Next Sessions